PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-108205
(43)Date of publication of application : 10.04.2002

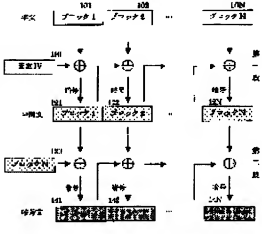
(51)Int.Cl. G09C 1/00

(21)Application number : 2000-295520 (71)Applicant : HITACHI SOFTWARE ENG CO LTD
(22)Date of filing : 28.09.2000 (72)Inventor : SAMEJIMA YOSHIKI

(54) BLOCK CIPHERING METHOD AND DECODING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a block ciphering method and a decoding method by which the original data can hardly be guessed at the time of making large data into a block and ciphering them.
SOLUTION: The ciphering stage of input data is constituted of at least two stages. Data is ciphered by using a password sentence block link mode in the block unit of prescribed byte length in the respective ciphering stages. In the initial ciphering stage, a fixed initialization vector which does not depend on input data is used and the ciphering result of one block in the previous ciphering stage is used as the initialization vector in the next and subsequent ciphering stages.

図1



LEGAL STATUS

[Date of request for examination] 08.10.2002
[Date of sending the examiner's decision of rejection] 13.12.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－108205
（P2002－108205A）
(43)公開日　平成14年４月10日(2002.4.10)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ａ　５Ｊ１０４

審査請求　未請求　請求項の数４　ＯＬ　（全４頁）

(21)出願番号　特願2000－295520(P2000－295520)

(22)出願日　平成12年９月28日(2000.9.28)

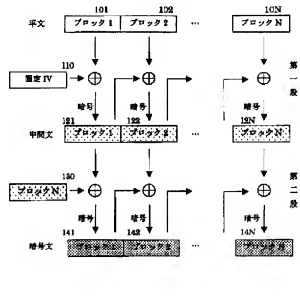
(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　鮫島　吉昇
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100088720
弁理士　小川　眞一

Ｆターム(参考)　5J104 AA16 EA04 JA03 NA02 NA04

(54)【発明の名称】　ブロック暗号方法及び復号方法

(57)【要約】
【課題】　大きなデータをブロック化して暗号化する際に、元のデータが推測されるのを困難にすることができるブロック暗号方法及び復号方法を提供すること。
【解決手段】　入力データの暗号化段階を少なくとも２つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における１つのブロックの暗号結果を初期化ベクトルとして用いる。

図１



1

【特許請求の範囲】

【請求項１】　入力データを所定バイト長のブロック単位で暗号化するブロック暗号方法において、

入力データの暗号化段階を少なくとも２つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における１つのブロックの暗号結果を初期化ベクトルとして用いることを特徴とするブロック暗号方法。

【請求項２】　前記最初の暗号化段階以降に用いる初期化ベクトルとして、前の暗号化段階における最後のブロックの暗号結果を用いることを特徴とする請求項１に記載のブロック暗号方法。

【請求項３】　所定バイト長のブロック単位で暗号化されたデータを復号するブロック暗号復号方法において、復号対象の入力データの復号段階を少なくとも２つの段階で構成し、かつ最後の暗号化段階から最初の暗号化段階に向かう順で復号し、最初の復号段階から最後の復号段階の１つ前までの復号段階では次に行う復号段階における１つのブロックの暗号結果を初期化ベクトルとして用い、最後の復号段階では固定の初期化ベクトルを用いることを特徴とするブロック暗号復号方法。

【請求項４】　前記最初の復号段階から最後の復号段階の１つ前までの復号段階で用いる初期化ベクトルとして、次の復号段階における大ブロック内の最後のブロックの暗号結果を用いることを特徴とする請求項３に記載のブロック暗号復号方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ブロック暗号方法および復号方法に関するものである。

【０００２】

【従来の技術】既存の秘密鍵暗号の暗号単位は、８バイト程度と比較的小さい。５１２バイト程度の大きなデータを暗号化する場合には、一般にＣＢＣモード（cipher block chaining モード；暗号文ブロック連鎖）といわれる方法で暗号化している。図４にその概要を示す。

【０００３】図４において、暗号化対象の平文（入力データ）は、例えば８バイト単位のブロック１（４０１）～Ｎ（４０Ｎ）に分割される。平文のブロック１（４０１）を暗号化するには、ブロック１（４０１）と初期化ベクタ（ＩＶ）と呼ばれるパラメータとの排他的論理和を暗号化し、暗号化されたブロック１（４２１）を得る。次に、平文のブロック２（４０２）を暗号化するが、この場合には、暗号化したブロック１（４２１）とブロック２（４０２）との排他的論理和を暗号化する。以下これを繰り返す。ブロックＮ（４０Ｎ）を暗号化するには、暗号化したブロックＮ－１と平文のブロックＮ（４０Ｎ）との排他的論理和を暗号化する。

2

【０００４】

【発明が解決しようとする課題】ＣＢＣモードでは、大きなデータの最初のブロックがいくつか同じであれば、暗号文の最初のいくつかのブロックも同じになってしまい、元のデータが推測され、解読される可能性が大きくなる。例えば、データＡとデータＢとでブロック１、ブロック２が同じであり、ブロック３が異なっていた場合、暗号文のブロック１とブロック２が同じになってしまう。

【０００５】本発明は、大きなデータをブロック化して暗号化する際に、元のデータが推測されるのを困難にすることができるブロック暗号方法及び復号方法を提供することにある。

【０００６】

【課題を解決するための手段】上記課題を解決するために、本発明のブロック暗号方法は、入力データの暗号化段階を少なくとも２つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における１つのブロックの暗号結果を初期化ベクトルとして用いることを特徴とする。

【０００７】また、前記最初の暗号化段階以降に用いる初期化ベクトルとして、前の暗号化段階における最後のブロックの暗号結果を用いることを特徴とする。

【０００８】また、本発明のブロック暗号復号方法は、所定バイト長のブロック単位で暗号化されたデータを復号するブロック暗号復号方法において、復号対象の入力データの復号段階を少なくとも２つの段階で構成し、かつ最後の暗号化段階から最初の暗号化段階に向かう順で復号し、最初の復号段階から最後の復号段階の１つ前までの復号段階では次に行う復号段階における１つのブロックの暗号結果を初期化ベクトルとして用い、最後の復号段階では固定の初期化ベクトルを用いることを特徴とする。

【０００９】また、前記最初の復号段階から最後の復号段階の１つ前までの復号段階で用いる初期化ベクトルとして、次の復号段階における大ブロック内の最後のブロックの暗号結果を用いることを特徴とする。

【００１０】

【発明の実施の形態】以下、本発明を図示する実施形態に従い詳細に説明する。図１は、本発明のブロック暗号方法の概要を示す図である。本発明では、入力データの暗号化段階を少なくとも２つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における１つのブロックの暗号結果を初期化ベクトルとして用い

る。

【００１１】図１の例では、説明を簡単にするために、暗号化段落を２段階にした例を示している。そして、最初の暗号化段落以降（２段階目の暗号化段階）に用いる初期化ベクトルとして、前の暗号化段階（最初の暗号化段階）における次ブロック内の最後のブロックＮの暗号結果を用いる例を示している。この場合、最後のブロックＮの暗号結果を用いる代わりに、ブロックＮの暗号結果を基に生成した初期化ベクトル、あるいは他のブロックの暗号結果を用いることもできる。ただし、最後のブロックＮの暗号結果を用いた方が暗号強度は強くなる。

【００１２】図１において、１０１～１０Ｎは、平文のブロック１からブロックＮ、１１０は固定の初期化ベクトル（ＩＶ）を示す。このＩＶ（１１０）は固定にしてもよいし、システム全体で固定してもよい。１２１～１２Ｎは、中間文のブロック１～ブロックＮ、１３０はブロックＮ（１２Ｎ）と同一であり、二段目の暗号化段階で使用する初期化ベクトルとなる。１４１～１４Ｎまでは、暗号文のブロック１からブロックＮである。

【００１３】図１で示す暗号化方法は、２段落の暗号化段落からなり、途中で中間文のブロック１（１２１）～ブロックＮ（１２Ｎ）を生成する。ブロック１（１０１）～ブロックＮ（１０Ｎ）から成る平文を暗号して中間文を生成するには、平文に依存しない固定の初期化ベクトル（１１０）を用いて先に説明したＣＢＣモードを用いて暗号化する。次に、中間文、その中間文のブロックＮ（１２Ｎ）を初期化ベクトル（１３０）として用い、ＣＢＣモードで暗号化して、ブロック１（１４１）～ブロックＮ（１４Ｎ）から成る最終の暗号文を得る。なお、ここで、最初の秘密鍵暗号と次の秘密鍵暗号の方法は異なっていてもよい。

【００１４】図２に、図１で説明した暗号化方法の処理手順をフローチャートにより示している。本発明のブロック暗号方法及び復号方法は、特に図示しないが、コンピュータとそのハードウェア資源を用いて実施するものである。図２において、まず、ステップ２０１で固定の初期化ベクトル（１１０）を用い、ブロック１（１０１）～ブロックＮ（１０Ｎ）から成る平文をＣＢＣモードで第一段の秘密鍵暗号にしたがって暗号化し、ブロック１（１２１）～ブロックＮ（１２Ｎ）から成る中間文を得る。すなわち、ブロック１（１０１）と固定の初期化ベクトル（１１０）の排他的論理和を暗号化して中間文のブロック１（１２１）を得る。次に平文のブロック（１０２）と中間文のブロック１（１２１）の排他的論理和を第一段の秘密鍵暗号にしたがって暗号化し、中間文のブロック２（１２２）を得る。以下これを繰り返し、中間文のブロックＮ（１２Ｎ）を得る。

【００１５】次に、ステップ２０２において、中間文のブロックＮ（１２Ｎ）を初期化ベクトル（１３０）として用い、ブロック１（１２１）～ブロックＮ（１２Ｎ）から成る中間文をＣＢＣモードで第二段の秘密鍵暗号にしたがって暗号化し、最終の暗号文を得る。すなわち、中間文のブロック１（１２１）と初期化ベクトル（１３０）の排他的論理和を第二段の秘密鍵暗号にしたがって暗号化して最終の暗号文のブロック１（１４１）を得る。次に、中間文のブロック２（１２２）と最終の暗号文のブロック１（１４１）の排他的論理和を第二段の秘密鍵暗号にしたがって暗号化してブロック２（１４２）を得る。以下これを繰り返し、最終の暗号文のブロックＮ（１４Ｎ）を得る。

【００１６】次に、図３のフローチャートを用いて復号処理について説明する。まずステップ３０１において、最終の暗号文のブロックＮ（１４Ｎ）を第二段の秘密鍵暗号にしたがって復号し、中間文のブロックＮ（１２Ｎ）を得る。

【００１７】次にステップ３０２において、ブロックＮ（１２Ｎ）と同一の初期化ベクトル（１３０）を用い、最終の暗号文をＣＢＣモードで第二段の秘密鍵暗号にしたがって復号し、中間文を得る。すなわち、ブロック（１４１）を第二段の秘密鍵暗号にしたがって復号し、初期化ベクトル（１３０）との排他的論理和をとり、ブロック（１２１）を得る。次に、ブロック２（１４２）を第二段の秘密鍵暗号にしたがって復号し、ブロック（１４１）との排他的論理和をとり、ブロック（１２２）を得る。以下これを繰り返し、ブロック１（１２１）～ブロックＮ（１２Ｎ）から成る中間文を得る。

【００１８】次に、ステップ３０３において、固定の初期化ベクトル（１１０）を用い、中間文をＣＢＣモードで第一段の秘密鍵暗号にしたがって復号し、ブロック１（１０１）～ブロックＮ（１０Ｎ）から成る平文を得る。すなわち、ブロック（１２１）を第一段の秘密鍵暗号にしたがって復号し、ブロック（１１０）との排他的論理和をとり、ブロック（１０１）を得る。次に、ブロック（１２２）を第一段の秘密鍵暗号にしたがって復号し、ブロック（１２１）の排他的論理和をとり、ブロック（１０２）を得る。以下これを繰り返し、ブロック（１０Ｎ）を得、最終の平文を得る。

【００１９】

【発明の効果】以上説明した本発明によれば、例えば５１２バイト長などの比較的大きなデータを安全に暗号化することができる。すなわち、５１２バイト長などの比較的大きなデータでは、最初のブロックに同じデータが存在することがあるが、本発明によれば、第二段の暗号化段階で平文に応じて異なる初期化ベクトルを用いて暗号化するので、異なる暗号文を得ることができ、解読を困難にすることができる。

【図面の簡単な説明】

【図１】本発明のブロック暗号方法の概要を示す図である。

【図２】本発明のブロック暗号方法の処理手順を示すフ

ローチャートである。

【図３】本発明のブロック暗号復号方法の処理手順を示すフローチャートである。

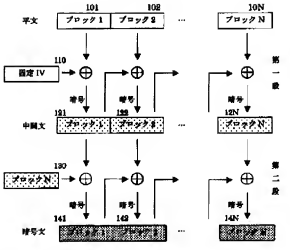
【図４】従来のブロック暗号方法の概要を示す図である。

＊【符号の説明】

１０１～１０Ｎ…平文のブロック、１１０…固定の初期化ベクトル、１２１～１２Ｎ…中間分のブロック、１４１～１４Ｎ…暗号文のブロック。

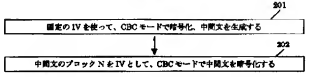
【図１】

図１



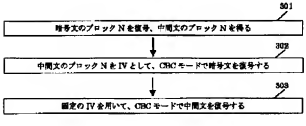
【図２】

図２



【図３】

図３



【図４】

図４